UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/890,587	11/07/2001	Micheal Maillard	11345/034001	6310

22511 7590 12/06/2005

OSHA LIANG L.L.P.
1221 MCKINNEY STREET
SUITE 2800
HOUSTON, TX 77010

EXAMINER	
MOORTHY, ARAVIND K	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 12/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/890,587	**Applicant(s)** MAILLARD, MICHEAL	
	Examiner Aravind K. Moorthy	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _07 September 2005_.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-9,12-15,17,21-25,28 and 31_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-9,12-15,17,21-25,28 and 31_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _07 November 2001_ is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed on 7 September 2005.

2. Claims 1-9, 12-15, 17, 21-25, 28 and 31 are pending in the application.

3. Claims 1-9, 12-15, 17, 21-25, 28 and 31 have been rejected.

4. Claims 10, 11, 16, 18-20, 26, 27, 29, 30, 32 and 33 have been cancelled.

5. Claims 14 and 15 have been objected to.

Response to Amendment

6. The examiner approves the amendment made to the specification. The applicant has included an abstract of the disclosure as required by 37 CFR 1.72(b).

7. The examiner approves of the amendment made to claims 6-20 and 24-31. Since claims 10, 11, 16, 18-20, 26, 27, 29 and 30 have been cancelled, they no longer have improper dependency. Claims 6-9, 12-15, 24, 25 and 28 have been amended so that they no longer conform to improper dependency.

8. Claims 32 and 33 have been cancelled. Therefore, they are no longer an omnibus type claim.

Claim Objections

9. Claims 14 and 15 are objected to because of the following informalities: improper dependency. Claims 14 and 15 depend upon claim 10. Claim 10 is a cancelled claim. A claim cannot depend upon a cancelled claim. For the sake of examination, the examiner assumes that claims 14 and 15 depend upon claim 1. Appropriate correction is required.

Response to Arguments

10. Applicant's arguments with respect to claims 1-9, 12-15, 17, 21-25, 28 and 31 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

11. Claims 1-5, 21 and 22 are rejected under 35 U.S.C. 102(b) as being anticipated by Wasilewski et al U.S. Patent No. 5,870,474.

As to claim 1, Wasilewski et al discloses a method of encryption of data in a digital television system communicated between a first decoder and a portable security module [column 7, lines 29-54]. Wasilewski et al discloses that at least one precalculated key pair is stored in a memory of the first decoder [column 8, lines 31-60]. Wasilewski et al discloses that the at least one key pair comprising a session key and an encrypted version of the session key prepared using a transport key [column 7 line 64 to column 8 line 7]. Wasilewski et al discloses the encrypted version of the session key being subsequently communicated to the portable security module which decrypts the encrypted version using an equivalent transport key stored in its memory such that data communicated from at least the portable security module to the first decoder may thereafter be encrypted and decrypted by the session key [column 7 line 64 to column 8 line 7].

As to claims 2 and 22, Wasilewski et al discloses a plurality of key pairs are stored in the memory of the first decoder [column 8, lines 31-60]. Wasilewski et al discloses the first decoder selecting and processing at least one session key to generate a definitive session key and communicating the associated encrypted version of the at least one session key to the portable security module for decryption and processing by the portable security module to generate the definitive session key [column 7 line 64 to column 8 line 7].

As to claim 3, Wasilewski et al discloses that a subset of a plurality of stored session keys is chosen by the first decoder to generate the definitive session key [column 7 line 64 to column 8 line 7]. Wasilewski et al discloses that the associated encrypted versions of the subset of session keys being communicated to the portable security module for decryption and processing [column 7 line 64 to column 8 line 7].

As to claim 4, Wasilewski et al discloses the order of combination of a plurality of session keys used to generate the definitive session key is communicated from the first decoder to the portable security device [column 7 line 64 to column 8 line 7].

As to claim 5, Wasilewski et al discloses an initial session key value known to both the first decoder and the portable security module is repeatedly encrypted in both devices by an ordered sequence of session keys using an encryption algorithm sensitive to the order of encryption [column 7 line 64 to column 8 line 7].

As to claim 6, Wasilewski et al discloses that at least one precalculated key pair is selected from a larger set of precalculated key pairs prior to being stored in the first decoder [column 8, lines 31-60].

As to claim 7, Wasilewski et al discloses that the encrypted version of a session key communicated to the portable security module also includes a signature value readable by the portable security module to verify the authenticity of the encrypted version of the session key [column 10 line 59 to column 11 line 9].

As to claim 12, Wasilewski et al discloses that the portable security module corresponds to one of a smart card and a conditional access module [column 12, lines 20-42].

As to claim 13, Wasilewski et al discloses that the first decoder corresponds to a conditional access module and the portable security module corresponds to a smart card [column 12, lines 20-42].

As to claim 14, Wasilewski et al discloses that data encrypted and decrypted with a session key corresponds to control word data [column 9, lines 31-46].

As to claim 15, Wasilewski et al discloses that data encrypted and decrypted with a session key corresponds to descrambled broadcast data [column 7 line 64 to column 8 line 7].

As to claim 17, Wasilewski et al discloses a home network system, wherein the first decoder and the portable security module corresponding to consumer electronic devices adapted to transfer data via a communication link [column 5, lines 23-46].

As to claim 21, Wasilewski et al discloses digital television system for providing secure communication of data between a first decoder and a portable security module [column 7, lines 29-54]. Wasilewski et al discloses that at least one precalculated key pair is stored in a memory of the first decoder [column 8, lines 31-60]. Wasilewski et al discloses that the at least one key pair comprising a session key and an encrypted version of the session key prepared using a transport key [column 7 line 64 to column 8 line 7]. Wasilewski et al discloses the encrypted version of the session key being subsequently communicated to the portable security module which decrypts the encrypted version using an equivalent transport key stored in its memory such that data communicated from at least the portable security module to the first decoder may thereafter be encrypted and decrypted by the session key [column 7 line 64 to column 8 line 7].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claims 8 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski et al U.S. Patent No. 5,870,474 as applied to claims 1 and 21 above, and further in view of Applied Cryptography (hereinafter Schneier).

As to claims 8 and 24, Wasilewski et al does not teach that that an algorithm and transport key used to encrypt and decrypt a session key corresponds to a symmetric algorithm and associated symmetric key.

Schneier teaches the use and benefits of symmetric key algorithms [page 216].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Wasilewski et al so that a symmetric algorithm and associated symmetric key would have been used to encrypt and decrypt a session key.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Wasilewski et al by the teaching of Schneier because symmetric key cryptography is magnitude faster and is not susceptible to chose-ciphertext attacks [page 216].

13. Claims 9 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski et al U.S. Patent No. 5,870,474 as applied to claims 1 and 21 above, and further in view of Applied Cryptography (hereinafter Schneier).

As to claim 9, Wasilewski et al does not teach that an encryption algorithm used with a session key to encrypt and decrypt data communicated between the first decoder and the portable security module corresponds to a symmetric algorithm.

Schneier teaches the use and benefits of symmetric key algorithms [page 216].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Wasilewski et al so that a symmetric key algorithm would have been used by the session key to encrypt and decrypt data communicated between the decoder and the portable security module.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Wasilewski et al by the teaching of Schneier because symmetric key cryptography is magnitude faster and is not susceptible to chose-ciphertext attacks [page 216].

14. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski et al U.S. Patent No. 5,870,474 as applied to claim 21 above, and further in view of Shwed et al U.S. Patent No. 5,835,726.

As to claim 23, Wasilewski et al does not teach that the encrypted version of a session key includes a signature value readable by the second device to verify the authenticity of the encrypted version of the session key.

Shwed et al teaches an encrypted version of a session key that includes a signature value readable by the portable security module to verify the authenticity of the encrypted version of the session key [column 17, lines 9-36].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Wasilewski et al so that the encrypted version of the session key would have included a signature valued used to verify the authenticity of the encrypted version of the session key.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Wasilewski et al by the teaching of Shwed et al because the signature provides authentication to the source that the key received is indeed formed by an entity that knows the basic key thus providing strong authentication [column 17, lines 9-36].

Conclusion

15. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy AM
November 30, 2005

Primary Examiner
AU2131
12/1/05